Finite Fields and Their Applications 48 (2017) 43–59

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On the dimension of twisted centralizer codes

Adel Alahmadi [b], S.P. Glasby [a,*,1], Cheryl E. Praeger [a,2]

[a] *Centre for Mathematics of Symmetry and Computation, University of Western Australia, 35 Stirling Highway, Crawley 6009, Australia*
[b] *Dept. of Mathematics, King Abdulaziz University, Jeddah, Saudi Arabia*

ARTICLE INFO

Article history:
Received 1 August 2016
Received in revised form 14 July 2017
Accepted 19 July 2017
Available online xxxx
Communicated by L. Storme

MSC:
primary 94B65
secondary 60C05

Keywords:
Dimension
Linear code
Twisted centralizer code

ABSTRACT

Given a field F, a scalar $\lambda \in F$ and a matrix $A \in F^{n\times n}$, the *twisted centralizer code* $C_F(A,\lambda) := \{B \in F^{n\times n} \mid AB - \lambda BA = 0\}$ is a linear code of length n^2 over F. When A is cyclic and $\lambda \neq 0$ we prove that $\dim C_F(A,\lambda) = \deg(\gcd(c_A(t), \lambda^n c_A(\lambda^{-1}t)))$ where $c_A(t)$ denotes the characteristic polynomial of A. We also show how $C_F(A,\lambda)$ decomposes, and we estimate the probability that $C_F(A,\lambda)$ is nonzero when $|F|$ is finite. Finally, we prove $\dim C_F(A,\lambda) \leqslant n^2/2$ for $\lambda \notin \{0,1\}$ and 'almost all' $n \times n$ matrices A over F.

* Corresponding author.
E-mail addresses: Stephen.Glasby@uwa.edu.au (S.P. Glasby), Cheryl.Praeger@uwa.edu.au (C.E. Praeger).
URLs: http://www.maths.uwa.edu.au/~glasby/ (S.P. Glasby), http://www.maths.uwa.edu.au/~praeger (C.E. Praeger).
[1] Also affiliated with The Department of Mathematics, University of Canberra, ACT 2601, Australia.
[2] Also affiliated with King Abdulaziz University, Jeddah, Saudi Arabia.

http://dx.doi.org/10.1016/j.ffa.2017.07.005

1. Introduction

Fix a (commutative) field F, a scalar $\lambda \in F$, and a matrix $A \in F^{n\times n}$. The subspace

$$C_F(A,\lambda) := \{B \in F^{n\times n} \mid AB - \lambda BA = 0\}$$

is called a *twisted centralizer code*. We are primarily interested in the case when $F = \mathbb{F}_q$ is a finite field, in which case $C_F(A,\lambda)$ is a linear code. This paper is motivated by results in [3]. We rely heavily on the fact that replacing A by a conjugate does not change $\dim C_F(A,\lambda)$. By contrast, the Hamming weight of a matrix (the number of nonzero entries), is highly sensitive to change of basis. Coding theory applications are considered in [4].

Let $c_A(t)$ be the characteristic polynomial of A, namely $\det(tI - A)$, and let $m_A(t)$ be its minimal polynomial. Let $\overline{F}$ be the algebraic closure of F. Let $S(A)$ denote the set of roots of $m_A(t)$ and hence also of $c_A(t)$ in $\overline{F}$, and let L be the subfield of $\overline{F}$ containing $S(A)$ and F, i.e. the splitting (sub)field for $c_A(t)$. Suppose $c_A(t) = \prod_{\alpha\in S(A)}(t-\alpha)^{m_\alpha}$ for positive integers m_α. View L^n as a right $L[A]$-module (usually as n-dimensional row vectors over L). For $\alpha \in L$ let K_α be the α-eigenspace $\{v \in L^n \mid vA = \alpha v\}$, and set $k_\alpha = \dim(K_\alpha)$. Note that $K_\alpha \neq \{0\}$ if and only if $\alpha \in S(A)$. Thus, in particular, K_0 is the row null space of A which we also denote $\mathrm{RNull}_L(A)$, and k_0 is the nullity of A. The $(t-\alpha)$-primary $L[A]$-submodule of L^n is $M_\alpha = \{v \in L^n \mid v(A-\alpha I)^n = 0\}$. Observe that $\dim(M_\alpha) = m_\alpha$ and $K_\alpha \leqslant M_\alpha$, so that $k_\alpha \leqslant m_\alpha$. To stress the dependence on A, we write $K_{A,\alpha}, k_{A,\alpha}, M_{A,\alpha}, m_{A,\alpha}$. When $\lambda = 1$, we write $C_F(A)$ instead of $C_F(A,1)$. Note that $C_F(A,\lambda)$ is a module for the F-algebra $C_F(A)$.

In Section 2 we see how $C_F(A,\lambda)$ decomposes, and in Section 3 we identify $C_F(A,\lambda)$ with the null space of a (parity check) matrix. When $\lambda \neq 0$, the 'λ-twisted' characteristic polynomial $\lambda^n c_A(\lambda^{-1}t)$ is closely related to $\dim C_F(A,\lambda)$. In Section 4 we prove that $\dim C_F(A,\lambda) = \deg(\gcd(c_A(t), \lambda^n c_A(\lambda^{-1}t)))$ when A is cyclic and $\lambda \neq 0$. If $\lambda \neq 0$ then $C_F(A,\lambda) \cong C_F(A_{\mathrm{nil}},\lambda) \oplus C_F(A_{\mathrm{inv}},\lambda)$ by Theorem 2.2 where A_{nil} and A_{inv} denote the 'nilpotent and invertible parts' of A. Theorem 2.4 gives a decomposition of $C_L(A,\lambda)$ related to the $(t-\alpha)$-primary $L[A]$-submodules of L^n provided F has prime characteristic, and a certain condition holds involving $\lambda^n c_A(\lambda^{-1}t)$ and $\lambda^{-n}c_A(\lambda t)$.

If $\det(A) = 0$, then $C_F(A,\lambda) \neq \{0\}$ for all $\lambda \in F$ by Corollary 2.7. In Section 5 we show when $\lambda \notin \{0,1\}$ that the probability is positive, that a uniformly distributed $A \in \mathbb{F}_q^{n\times n}$ has $C_{\mathbb{F}_q}(A,\lambda) \neq \{0\}$. In Section 6 we establish upper bounds for $\dim C_F(A,\lambda)$, and Theorem 6.2 proves that $\lambda \notin \{0,1\}$ and $k_0 + m_0/2 \leqslant n$ implies that $\dim C_F(A,\lambda) \leqslant n^2/2$. The bound $n^2/2$ is attained when n is even and $\lambda = -1$ by Remark 6.4.

2. The nilpotent and invertible parts of A

A matrix $A \in F^{n\times n}$ is called *nilpotent* if $A^n = 0$. The n-dimensional row space $V = F^n$ decomposes as $V = V_{\mathrm{nil}} \oplus V_{\mathrm{inv}}$ where